

# **LLNL Computer Use Policy and Security Rules**

**CSP2329 V2.1**

**5/21/97**

***Lawrence Livermore National Laboratory***

# **LLNL Computer Use Policy and Security Rules**

Line managers are responsible for implementing this policy and rules in their organization and ensuring that users are aware of their responsibilities. This requirement applies to both classified and unclassified operations. All personnel should retain a copy for reference and audit purposes.

Computers and network systems are inherently insecure. All personnel, and particularly users, are cautioned that in general these technologies are not "private." Therefore users should not "automatically" expect privacy when using systems or networks. Take appropriate protective measures, protecting sensitive information and applications accordingly. This list represents LLNL minimum requirements, your management may have additional requirements. Questions concerning these rules should be addressed to your supervisor, manager, or CSSO.

## **Computer Use:**

LLNL computer systems and communications networks are funded by the United States government for the purpose of supporting the Laboratory's programmatic and business activities. These controlled government resources are to be used for official business only. In addition to the use of computers on site, this policy applies to the use of government-owned computers at locations other than the Laboratory premises and the use of communication networks funded by the government. Because these are government resources, the Laboratory or an agent of the federal government may at any time and without notice audit or access any LLNL computer system connected to or using Laboratory-funded data communications. Any information obtained through such auditing may be disclosed to third parties, including law enforcement authorities.

## **LLNL (University of California) employees:**

Minor incidental personal use is allowed if it satisfies the following criteria:

It is supportive of the intent of Contract 48 between the University of California and the Department of Energy;

It does not involve illegal activities;

It does not involve personal gain;

It does not violate LLNL policy;

It does not involve any activity which will potentially embarrass the Laboratory, DOE or the loss of public trust and

It does not involve any unauthorized activity which impacts or interferes with an employee's legitimate job performance.

This policy does not authorize incidental personal use in support of non-LLNL external organizations.

Information accessed through the World Wide Web (WWW) with the use of LLNL computers and communication networks is restricted to that which is work related. Incidental personal use of information for education and professional development reasons is permitted.

If there are any questions as to whether or not an employee's use meets these criteria, the employee should contact his or her supervisor for clarification. Supervisors may contact the Computer Security Organization if further guidance is necessary.

Employees are reminded that any use of LLNL computers and communication networks by individuals other than LLNL and DOE employees continues to be prohibited. Employees are also reminded that when they use a LLNL computer or network resource, they are acting in their capacity as LLNL employees. E-mail sent from a Laboratory network always bears the address "llnl.gov". Messages and postings at news groups and other locations on the World Wide Web also bear the llnl.gov source address.

## **Non-LLNL (University of California) employees:**

Computers, software, and communications systems provided by LLNL are to be used only for work related purposes (as determined by the responsible manager). The use of this equipment or software for personal or non-work related activity is prohibited.

**User Accountability:** Users are accountable for their actions and may be held liable to administrative or criminal sanctions for any unauthorized actions found to be intentional, malicious, or grossly negligent.

**Unauthorized Access:** Users are not to access or attempt to access systems or information for which they are not authorized. Users are not to attempt to receive unintended messages or access information by some unauthorized means, such as imitating another system, impersonating another user or other person, misuse of legal user credentials (User IDs, passwords, etc.), or by causing some network component to function incorrectly. Users are not to possess or transfer information for which they are not authorized.

**Software License:** All software used on LLNL computers must be appropriately acquired and used according to the appropriate licensing. This means that any illegally copied software or use is expressly prohibited. Software used on classified systems must be approved (generically or specifically) by the appropriate CSSO.

**Passwords and User IDs:** A user identifier (name or employee number) known as a User ID and password are required of all users of a multi-user system (two or more users) *or* system allowing any access through a network or telephone line (modems). Passwords are protected commensurate (equal) to the data and system they protect. Passwords must be changed at least annually. Passwords must be at least six (6) characters long, not found in a dictionary, and cannot be the name of a person, place, or thing. Passwords must not be shared with any other person, except when necessary with the system Computer System Security Officer (CSSO) or by authority of the LLNL Computer Security Manager. The password must be changed as soon as possible after an unacceptable exposure or suspected compromise.

**Malicious Software:** Users must not introduce or use malicious software such as computer viruses, Trojan horses, or worms.

**Altering Authorized Access:** Users are prohibited from changing access controls to allow themselves or others to perform actions outside their authorized privileges.

**Denial of Service Actions:** Users are not allowed to prevent others or other systems from performing authorized functions by actions that deny their access, their communications capability, deliberately suppressing their messages or generating frivolous or unauthorized traffic.

**Data Modification or Destruction:** Users are prohibited from taking unauthorized actions to intentionally modify, delete information or programs.

**Reconstruction of Information or Software:** Users are not allowed to reconstruct or recreate information or software for which they are not authorized.

**Network Registration:** All network users (including user of Open LabNet) must be registered with their system administrator, CSSO, or as otherwise appropriate to that network's requirements.

**Modems, Dial-up, and Remote Access:** All dial-up devices (modems, etc.) must have password protection. All dial-up access through telephone lines (LLIX or analog) must be registered and approved by the responsible system or network administrator.

**Sensitive and Critical Operations:** Those users, and their systems, as determined by management to involve sensitive information *or* critical/essential operations must also follow the appropriate requirements from their management, based upon LLNL Computer Security organization guidance.

Violation of these policies may lead to corrective action, up to and including dismissal.

### **Misuse, Abuse, and Criminal Activity**

All LLNL personnel, organizations, and subcontractors are responsible to address, safeguard against, and report misuse, abuse, and criminal activity. These activities should be reported to the Safeguards and Security (S&S) Department, Investigations Section. The LLNL Computer Security organization initiates and participates in appropriate investigative activities in concert with the Safeguards & Security Department.

The following general definitions may be helpful in recognizing reportable issues

- Misuse** Waste (activities that negatively impact system or work performance) of computer time or resources.
- Abuse** Intentional destruction, denial of service or use, unauthorized alteration of software, hardware or information, or intentional circumvention of security rules.
- Criminal** Illegal activities including fraud, personal gain, or copyright violations, etc.

### **Computer Security Assessment Teams**

Open LabNet, Closed LabNet, other LLNL networks, as well as computers, and users, will be assessed by the LLNL Computer Security Assessment Teams on a periodic and "for cause" basis.